

Certification PECB - Analyse de risques par la méthode MEHARI

CATEGORIE : B

Vue d'ensemble

Domaine(s) d'activité professionnel dans lequel(s) est utilisé la certification :

Transverse : ■ **Tous secteurs d'activité**

Code(s) NAF : **62.03Z**

Code(s) NSF : **326**

Code(s) ROME : **M1801**, **M1805**

Formacode : **31006**

Date de création de la certification : **01/03/2014**

Mots clés : **Cyber sécurité**, **Sécurité**,
Systèmes d'information, **Objectifs de sécurité**

Identification

Identifiant : **4319**

Version du : **19/12/2018**

Références

Consensus, reconnaissance ou recommandation :

Formalisé :

- [Livre blanc défense et sécurité nationale Mission confiée par le Président de la République à Jean-Marie GUEHENNO, Conseiller maître à la Cour des Comptes - 2013](#)

Non formalisé :

- [Agence nationale de la sécurité des systèmes d'information \(ANSSI\) Bonnes pratiques / 2009-2018](#)

Norme(s) associée(s) :

- https://www.iso.org/files/live/sites/isoorg/files/store/fr/PUB100427_fr.pdf

Descriptif

Objectifs de l'habilitation/certification

Adossée à la norme ISO 27005, la certification recouvre les compétences nécessaires pour l'analyse de risques relative à la sécurité de l'information par la méthode MEHARI (*M*éthode *H*armonisée d'*A*nalyse de *R*isques). Elle vise à doter les managers du cadre méthodologique et technique permettant d'identifier et de traiter les risques dans une perspective de prévention.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- Aucun

Descriptif général des compétences constituant la certification

La certification recouvre cinq compétences-clés :

Identifier et évaluer les dysfonctionnements potentiels du système d'information, afin de classer ceux-ci selon la méthode MEHARI sur une échelle de valeur traduisant les principaux enjeux de sécurité. Analyser les vulnérabilités dans tout le contexte de travail de

Public visé par la certification

Tous publics

l'entreprise, afin de corriger les points de faiblesse inacceptables par des plans d'action immédiats et conformes à la norme ISO 27005.
Prendre en compte le système d'information au sens large et tous types d'information afin de créer une base de connaissances complète et experte en matière de sécurité conforme à la norme ISO 27005.
Analyser et évaluer les situations de risque pour l'entreprise afin de déterminer leur probabilité d'occurrence, en vue de mettre en évidence des mesures de sécurité conformes à la norme ISO 27005 et susceptibles de ramener les risques à un niveau acceptable.
Piloter la sécurité du système d'information grâce à des indicateurs et des références externes, en vue de réduire les écarts entre les objectifs et les résultats.

Modalités générales

La formation conduisant à la certification est proposée en quatre journées (32 heures), en présentiel.

Cette formation est basée sur les meilleures pratiques en matière d'analyse de risques.

Les cours théoriques sont ponctués par de la mise en application. La répartition théorique et pratique est de 40-60%.

Les exercices pratiques sont panachés de travaux dirigés et guidés par l'apprenant et d'exercices en pleine autonomie, afin d'assurer une assimilation des savoir-faire requis.

Liens avec le développement durable

Aucun

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

La certification permet aux individus de :

Disposer des compétences nécessaires à la réalisation d'un programme d'analyse et de traitement des risques au sein de leur entreprise.
Appartenir au réseau de formateurs et certifiés PECB sollicités pour leurs compétences auprès des clients à l'international.
Répondre aux exigences de postes correspondant à ces caractéristiques : RSSI, responsable de la gestion des risques en sécurité de l'information, consultant en cyber sécurité, etc.

Pour l'entité utilisatrice

La multiplication des risques liés aux intrusions dans les systèmes d'information impose à toutes les entreprises de mettre en place des dispositifs de sécurité permettant d'assurer la continuité de leurs activités. La certification est adaptée à la nécessaire qualification de leurs managers à cette fin, dotant ceux-ci d'une méthodologie d'analyse internationalement reconnue.

La certification permet aux entités utilisatrices de :

Faciliter la gestion des compétences et le recrutement en s'appuyant sur une certification reconnue.
Favoriser la collaboration inter-organisationnelle en partageant un langage et des processus communs.
Garantir aux parties prenantes de l'organisation un certain standard de qualité.
Le maintien dans le temps de la certification garantit la transférabilité des compétences d'une entité utilisatrice à une autre.

Evaluation / certification

Pré-requis

Connaissances des principaux concepts de la norme ISO 27005.

Compétences évaluées

Evaluation de la totalité des cinq compétences-clés :

Identifier et évaluer les dysfonctionnements potentiels du système d'information, afin de classifier ceux-ci selon la méthode MEHARI sur une échelle de valeur traduisant les principaux enjeux de sécurité. Analyser les vulnérabilités dans tout le contexte de travail de l'entreprise, afin de corriger les points de faiblesse inacceptables par des plans d'action immédiats et conformes à la norme ISO 27005. Prendre en compte le système d'information au sens large et tous types d'information afin de créer une base de connaissances complète et experte en matière de sécurité conforme à la norme ISO 27005. Analyser et évaluer les situations de risque pour l'entreprise afin de déterminer leur probabilité d'occurrence, en vue de mettre en évidence des mesures de sécurité conformes à la norme ISO 27005 et susceptibles de ramener les risques à un niveau acceptable. Piloter la sécurité du système d'information grâce à des indicateurs et des références externes, en vue de réduire les écarts entre les objectifs et les résultats.

Niveaux délivrés le cas échéant (hors nomenclature des niveaux de formation de 1969)

Pas de niveau.

La validité est Temporaire

La certification est valable 3 années.

Possibilité de certification partielle : non

Matérialisation officielle de la certification :

Remise d'un certificat de compétences PECB sous accréditation IAS (ISO 17024)

Centre(s) de passage/certification

- Adenium (Paris)
- Devoteam (Paris - Bruxelles - Luxembourg)
- Fidens (Paris - Lyon)
- Global Knowledge (Rueil Malmaison)
- HTS Experts (Valencienne)
- It-Gnosis (Paris)
- Orsys (Paris-Bruxelles-Luxembourg-Genève)
- Provadys (Paris)
- SCASSI (Toulouse - Paris - Madrid)
- Sekoia (Paris)
- Sodifrance (Rennes - Nantes)
- Sysdream (Paris)

Plus d'informations

Statistiques

20 certificats sont délivrés en moyenne annuelle.

Autres sources d'information

<https://pecb.com/fr/education-and-certification-for-individuals/iso-iec-27005>